# Exhibit 4

Trials@uspto.gov
571-272-7822

Paper 12
Date: February 28, 2022

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

SAMSUNG ELECTRONICS AMERICA, INC.,
Petitioner,

v.

PROXENSE, LLC,
Patent Owner.

---

IPR2021-01447
Patent 9,298,905 B1

---

Before KEVIN F. TURNER, JUSTIN T. ARBES, and DAVID C. McKONE, *Administrative Patent Judges.*

TURNER, *Administrative Patent Judge*.

# DECISION
Denying Institution of *Inter Partes* Review
*35 U.S.C. § 314*

# I. INTRODUCTION

## A. *Background and Summary*

Petitioner Samsung Electronics America, Inc. filed a Petition (Paper 1, "Pet.") requesting *inter partes* review of claims 1–12 of U.S. Patent No. 9,298,905 B1 (Ex. 1001, "the '905 Patent") pursuant to 35 U.S.C. § 311(a). Patent Owner Proxense, LLC filed a Preliminary Response (Paper 10, "Prelim. Resp.") pursuant to 35 U.S.C. § 313.

Pursuant to 35 U.S.C. § 314(a), the Director may not authorize an *inter partes* review unless the information in the petition and preliminary response "shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." *See* 37 C.F.R. § 42.4(a) ("The Board institutes the trial on behalf of the Director."). For the reasons that follow, we do not institute an *inter partes* review.

## B. *Related Matters*

The parties indicate that the '905 Patent is the subject of *Proxense, LLC v. Samsung Electronics Co., Ltd.*, Case No. 6:21-cv-00210 (W.D. Tex.) ("the district court case"). *See* Pet. 3; Paper 5, 1. Petitioner also filed petitions challenging claims of other patents asserted in the district court case: Cases IPR2021-01438, IPR2021-01439, IPR2021-01444, and IPR2021-01448.

## C. *The '905 Patent*

The '905 Patent discloses systems for "authentication responsive to biometric verification of a user being authenticated," using "a persistent storage to persistently store[] a code such as a device identifier (ID) and biometric data for a user in a tamper-resistant format." Ex. 1001, 1:65–67.

The '905 Patent states that "[c]onventional user authentication techniques," such as requiring input of a password, were deficient because they "require[d] the user to memorize or otherwise keep track of the credentials" and "it can be quite difficult to keep track of them all." *Id.* at 1:28–37. Other techniques, such as "provid[ing] the user with an access object . . . that the user can present to obtain access," were inadequate because "authentication merely proves that the access object itself is valid; it does not verify that the legitimate user is using the access object." *Id.* at 1:38–46. According to the '905 Patent, there was a need in the art for a system for "verifying a user that is being authenticated that does not suffer from [such] limitations" and "ease[s] authentications by wirelessly providing an identification of the user." *Id.* at 1:55–58.

Figure 2 of the '905 Patent is reproduced below.

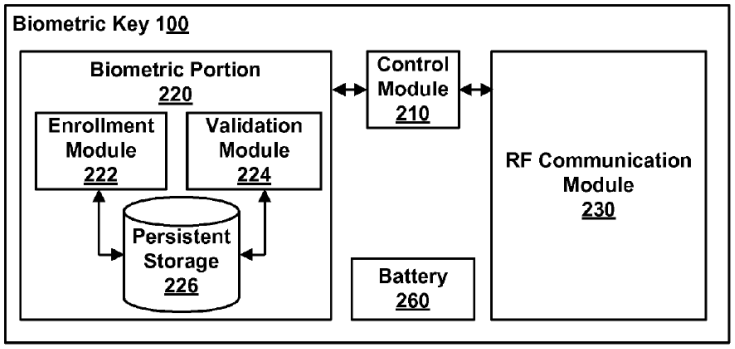


FIG. 2

Figure 2 is a block diagram of the functional modules of a biometric key. Ex. 1001, 3:30–33, 4:42–43. Enrollment module 222 registers a user with biometric key 100 by persistently storing biometric data associated with the user (e.g., a digital image of the retina, fingerprint, or voice sample) in persistent storage 226. *Id.* at 4:67–5:23. Enrollment module 222 registers biometric key 100 with a trusted authority by providing a code, such as a device ID, to the trusted authority or, alternatively, the trusted authority can

provide a code to biometric key 100. *Id.* at 5:3–7. The code is stored in persistent storage 226. *Id.* at 5:24–26. "Persistent storage 226 is itself, and stores data in, a tamper-proof format to prevent any changes to the stored data." *Id.* at 5:31–33. "Tamper-proofing increases reliability of authentication because it does not allow any changes to biometric data (i.e., allows reads of stored data, but not writes to store new data or modify existing data)." *Id.* at 5:33–36. In a fingerprint embodiment, validation module 224 uses scan pad 120 (shown in Figure 1) to capture scan data from the user's fingerprint and compares the scanned data to the stored fingerprint to determine whether the scanned data matches the stored data. *Id.* at 5:8–12.

The interaction of biometric key 100 with other system components is illustrated in Figure 3, reproduced below.

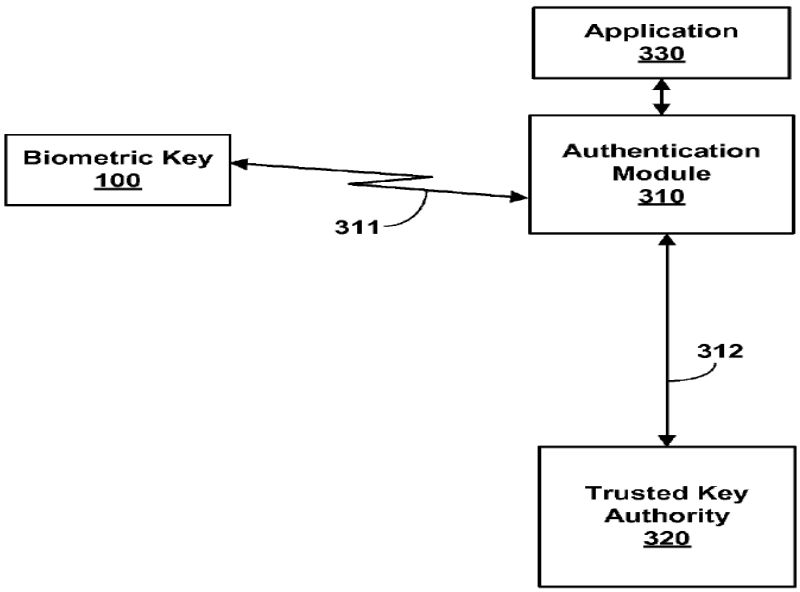


FIG. 3

Figure 3 is "a block diagram illustrating a system for providing authentication information for a biometrically verified user." Ex. 1001,

3:33–35. Authentication module 310 is coupled to biometric key 100 via line 311 (a wireless medium) and with trusted key authority 320 via line 312 (a secure data network such as the Internet). *Id.* at 5:67–6:7. Authentication module 310 requires the device ID code (indicating successful biometric verification) from biometric key 100 before allowing the user to access application 330. *Id.* at 6:10–13. Authentication module 310 provides the device ID code from biometric key 100 to trusted key authority 320 to verify that it belongs to a legitimate key. *Id.* at 6:13–19; *see also id.* 6:39–45 ("In one embodiment, trusted key authority 320 verifies that a code from a biometric key is legitimate. To do so, the trusted key authority 320 stores a list of codes for legitimate biometric keys. . . . In one embodiment, trusted key authority 320 can also store a profile associated with a biometric key."). Authentication module 310 then sends a message to application 330 to allow the user access to the application responsive to a successful authentication by trusted key authority 320. *Id.* at 6:17–19.

"Application 330 can be, for example, a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file, a financial account . . . and the like." Ex. 1001, 6:21–26. Trusted key authority 320 can be operated by an agent, such as "a government official, a notary, and/or an employee of a third party which operates the trusted key authority, or another form of witness." *Id.* at 7:33–36. "The agent can follow standardized procedures such as requiring identification based on a state issued driver license, or a federally issued passport in order to establish a true identity of the user." *Id.* at 7:36–39.

### *D. Illustrative Claim*

Challenged claims 1 and 9 of the '905 Patent are independent. Claims 2–8 and 10–12 depend directly or indirectly from claim 1, although the language of certain claims suggests that the Patentee may have intended certain claims to have different dependencies. *See* Pet. 34 (taking no position regarding potential indefiniteness due to the dependencies). Claims 13–18 also issued with the '905 Patent, but are not challenged.

Claim 1 recites (with letter designations used in the Petition (Pet. iv) to refer to the various limitations):

> 1. A method comprising:
>
> [A] persistently storing biometric data of a legitimate user and an ID code on an integrated device;
>
> [B] responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;
>
> [C] comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;
>
> [D] responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and
>
> [E] responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code, allowing the user to complete a financial transaction.

Ex. 1001, 10:11–28.

*E. Asserted Grounds of Unpatentability*

Petitioner asserts the following grounds of unpatentability (Pet. 5), supported by the declaration of Dr. Andrew Wolfe (Ex. 1003) in support of its contentions:

| Claim(s) Challenged | 35 U.S.C. § | References/Basis |
|---|---|---|
| 1, 3–10, 12 | 103(a)[1] | Scott[2], Lapsley[3] |
| 2, 11 | 103(a) | Scott, Lapsley, Robinson[4] |
| 1, 3–7, 9, 10, 12 | 103(a) | Berardi[5], Shreve[6], Kinoshita[7] |

[1] The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) ("AIA"), amended 35 U.S.C. § 103. Because the challenged claims of the '905 Patent have an effective filing date before the effective date of the applicable AIA amendment, we refer to the pre-AIA version of 35 U.S.C. § 103. *See* Ex. 1001, codes (22), (60).

[2] International Patent Application Publication No. WO 99/56429, published Nov. 4, 1999 (Ex. 1005, "Scott"); when referencing portions of Scott, we refer to the original publication's page numbers in the top-center of each page (not the page numbers added by Petitioner in the lower-right corner of each page), consistent with the parties' usage in their papers.

[3] US Patent Application Publication No. 2001/0000535 A1, published Apr. 26, 2001 (Ex. 1007, "Lapsley").

[4] US Patent Application Publication No. 2003/0177102 A1, published Sept. 18, 2003 (Ex. 1008, "Robinson").

[5] US Patent No. 7,239,226 B2, filed July 9, 2002, issued July 3, 2007 (Ex. 1010, "Berardi").

[6] US Patent Application Publication No. 2002/0109580 A1, published Aug. 15, 2002 (Ex. 1012, "Shreve").

[7] US Patent Application Publication No. 2003/0055792 A1, published Mar. 20, 2003 (Ex. 1013, "Kinoshita").

## II. ANALYSIS

### *A. Discretionary Denial Under 35 U.S.C. § 314(a)*

Institution of *inter partes* review is discretionary. *See Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1367 (Fed. Cir. 2016) ("[T]he PTO is permitted, but never compelled, to institute an [*inter partes* review (IPR)] proceeding."); 35 U.S.C. § 314(a) ("The Director *may not* authorize an inter partes review to be instituted unless the Director determines that the information presented in the petition filed under section 311 and any response filed under section 313 shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." (emphasis added)). In the Preliminary Response, Patent Owner argues that we should exercise our discretion to deny the Petition in view of the district court case, where Petitioner previously asserted that we should not exercise our discretion to deny institution. Prelim. Resp. 4–6; Pet. 13–19. We need not decide this issue, however, as we determine that Petitioner has not shown a reasonable likelihood that it would prevail with respect to at least one of the challenged claims.

### *B. Legal Standards*

A claim is unpatentable for obviousness if, to one of ordinary skill in the pertinent art, "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007) (quoting 35 U.S.C. § 103(a) (2006)). The question of obviousness is resolved on the basis of underlying factual determinations, including "the scope and content of the prior art"; "differences between the prior art and the claims at issue"; and "the level of

ordinary skill in the pertinent art." *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). Additionally, secondary considerations, such as "commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented. As indicia of obviousness or nonobviousness, these inquiries may have relevancy." *Id.* When conducting an obviousness analysis, we consider a prior art reference "not only for what it expressly teaches, but also for what it fairly suggests." *Bradium Techs. LLC v. Iancu*, 923 F.3d 1032, 1049 (Fed. Cir. 2019) (citation omitted).

A patent claim "is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art." *KSR*, 550 U.S. at 418. An obviousness determination requires finding "both 'that a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so.'" *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1367–68 (Fed. Cir. 2016) (citation omitted); *see KSR*, 550 U.S. at 418 (for an obviousness analysis, "it can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does").

"Although the *KSR* test is flexible, the Board 'must still be careful not to allow hindsight reconstruction of references . . . without any explanation as to *how* or *why* the references would be combined to produce the claimed invention.'" *TriVascular, Inc. v. Samuels*, 812 F.3d 1056, 1066 (Fed. Cir. 2016) (citation omitted). Further, an assertion of obviousness "cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal

conclusion of obviousness." *KSR*, 550 U.S. at 418 (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)); *accord In re NuVasive, Inc.*, 842 F.3d 1376, 1383 (Fed. Cir. 2016) (stating that "conclusory statements" amount to an "insufficient articulation[] of motivation to combine"; "instead, the finding must be supported by a 'reasoned explanation'" (citation omitted)); *In re Magnum Oil Tools Int'l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016) ("To satisfy its burden of proving obviousness, a petitioner cannot employ mere conclusory statements. The petitioner must instead articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness.").

### *C. Level of Ordinary Skill in the Art*

Petitioner argues that at the time of the '905 Patent, a person of ordinary skill in the art would have had "a bachelor's degree in computer or electrical engineering (or an equivalent degree) with at least three years of experience in the field of encryption and security (or an equivalent)." Pet. 4. Patent Owner does not address the level of ordinary skill in the art in its Preliminary Response. Based on the record presented, including our review of the '905 Patent and the types of problems and solutions described in the '905 Patent and cited prior art, we adopt Petitioner's definition of the level of ordinary skill in the art and apply it for purposes of this Decision.

### *D. Claim Interpretation*

We interpret the challenged claims

> using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.

37 C.F.R. § 42.100(b) (2021). "In determining the meaning of [a] disputed claim limitation, we look principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence." *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006). Claim terms are generally given their ordinary and customary meaning as would be understood by a person of ordinary skill in the art at the time of the invention and in the context of the entire patent disclosure. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (en banc). "There are only two exceptions to this general rule: 1) when a patentee sets out a definition and acts as his own lexicographer, or 2) when the patentee disavows the full scope of a claim term either in the specification or during prosecution." *Thorner v. Sony Comput. Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012).

Petitioner submits that no express interpretations of any claim terms are necessary to resolve the parties' dispute and "the claim terms should be given their plain and ordinary meaning." Pet. 7. Patent Owner identifies two claim terms, "third-party trusted authority" and "access message," both recited in independent claims 1 and 9, that it presents as being edifying, based on Petitioner's Opening Claim Construction Brief in the district court case (Ex. 2001), and its own Responsive Claim Construction Brief (Ex. 2002). Prelim. Resp. 2–4.

Patent Owner points out that Petitioner argued in the district court case that a "third-party" is "an entity with a responsibility separate from executing the transaction itself." Prelim. Resp. 2 (quoting Ex. 2001, 7). In the district court case, Petitioner argued that no construction of "third-party trusted authority" was needed and "[t]he intrinsic evidence does not suggest

a party or component numbered after a second party." Ex. 2001, 6–7. This was in response to its articulation of Patent Owner's position, namely, that a "third-party trusted authority" is "[a] third component that provides a second level of authentication." *Id.* at 6.[8]

Petitioner further argued that "[d]uring prosecution, the applicant explained a 'user []prov[ing] to the same institution that authenticates the fingerprint information that the user is who he purports to be' does not satisfy the 'third party' limitation," and "[t]he applicant emphasized the prior art 'disclose[d] two parties: the user and the institution.'" Ex. 2001, 7 (quoting remarks made by the applicant for a related patent accompanying an amendment and addressing the same claim term) (alterations by Petitioner). Petitioner argued that "the intrinsic evidence suggests 'third party' relates to a specific class of entity occupying the aforementioned particular relationship." *Id.* Petitioner then pointed out that "the [S]pecification [of the related patent] explains the agent for the trusted authority 'can be, for example, a government official, a notary, and/or an employee of a third party which operates the trusted key authority, or another form of witness.'" *Id.* According to Petitioner, "[t]his 'witness' role further aligns with prosecution history where the applicant explained 'sending a code to a receiver of a *door that the user is trying to access*' does not satisfy the 'third party' limitation." *Id.* (quoting an amendment in the related patent file history).

[8] In its responsive brief, Patent Owner changed its position with respect to the terms "third-party trusted authority" and "agent" to "[n]o construction needed" and stated that it "no longer seeks to submit th[e] term[s] for construction." Ex. 2002, 12. The district court did not construe the terms. Ex. 3001.

Petitioner further offered expert testimony in the district court case to support an argument that "[c]ommon industry use of 'trusted third party' identifies 'third party' as an entity with a responsibility separate from executing the transaction itself." *Id.* at 7–8 (citing a declaration of Seth James Nielson, Ph.D. (Ex. 2003 ¶¶ 70–74) and a book, CRYPTOGRAPHIC LIBRARIES FOR DEVELOPERS). Dr. Nielson appears to best articulate the distinction Petitioner was drawing between a third component and a third entity: "the [S]pecification, the prosecution history, and common industry usage all suggest a 'third party' refers to an entity outside of the transaction or a witness thereto rather than a 'third component.'" Ex. 2003 ¶ 74.

In light of Petitioner's arguments in the district court case, Patent Owner contends that the parties "agree that a 'third-party trusted authority' is an institution or entity that is outside of the multi-party system (user and application or vendor) that is being authenticated." Prelim. Resp. 3.

We agree with Patent Owner. The plain meaning of "third-party trusted authority" suggests an entity or party separate from the principal parties to a transaction. *See, e.g.*, THE AMERICAN HERITAGE COLLEGE DICTIONARY 1433 (4th ed. 2004) ("third party n. . . . 2. One other than the principals involved in a transaction.") (Ex. 3002).

This is consistent with the description in the Specification. For example, Figure 3, reproduced above, depicts trusted key authority 320 as an entity separate from biometric key 100, authentication module 310, and application 330. As the Specification states, "[t]rusted key authority 320 is a third-party authority that is present in some embodiments in order to provide enhanced security." Ex. 1001, 6:37–39. Examples of trusted key authorities include "a government official, a notary, and/or an employee of a third party which operates the trusted key authority, or another form of witness." *Id.* at

7:33–36. Petitioner's citations to the applicant's statement during prosecution of the related patent also are consistent with a third-party trusted authority being an entity separate from the principal parties to a transaction, as is the declaration of Dr. Nielson. *See* Ex. 2001, 6–8; Ex. 2003 ¶¶ 70–74. Thus, we interpret "third-party trusted authority" to mean a trusted authority that is an entity separate from the parties to a transaction.

Claim 1 also recites "responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code," with claim 9 providing a similar recitation. Patent Owner argues that "[a]n 'access message' must be sent by the 'third party trusted authority'" and the parties "agree that the 'access message' originates from the 'third-party trusted authority' and communicates information regarding authentication." Prelim. Resp. 3–4 (citing Ex. 2001, 9). Given the express requirement in claims 1 and 9 that the access message be received "from" the third-party trusted authority, we conclude that no further interpretation of the "access message" limitations is necessary.[9]

### *E. Obviousness Ground Based on Scott and Lapsley*

Petitioner contends that claims 1, 3–10, and 12 are unpatentable over Scott and Lapsley under 35 U.S.C. § 103(a). Pet. 19–34. Patent Owner argues that the Petition fails to demonstrate that the combination of references teaches or suggests all elements of the challenged claims. Prelim.

[9] Petitioner argued in the district court case that the limitations mean "[r]eceiving a signal from the agent permitting a user to access an application," Patent Owner argued that no construction was necessary and the phrases should be given their plain and ordinary meaning, and the district court determined that no construction was necessary. Ex. 3001, 3.

Resp. 6–9. We are not persuaded that Petitioner has established a reasonable likelihood of prevailing on this asserted ground as to any of the challenged claims. We begin with short discussions of Scott and Lapsley, and discuss Petitioner's contentions and Patent Owner's arguments thereafter.

*1. Scott*

Scott describes "a portable personal identification device for providing secure access to a host facility" in which the device "includes a biometric sensor system capable of sensing a biometric trait of a user that is unique to the user and provid[es] a biometric signal indicative thereof." Ex. 1005, 2:5–8. Figure 1 of Scott, reproduced below, illustrates an example.

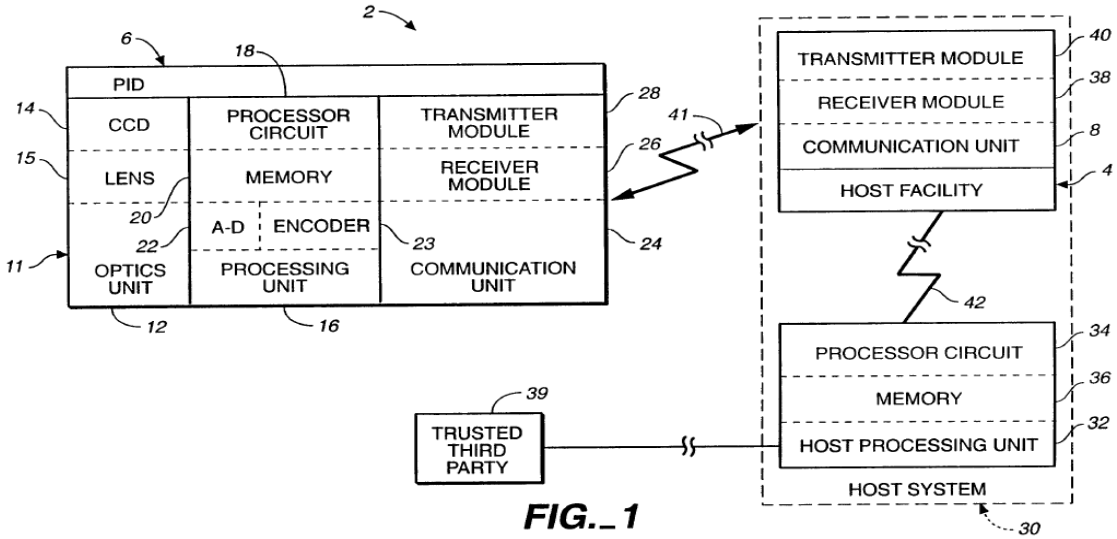


FIG._1

Figure 1 is a block diagram of security system 2 that provides access to host facility 4 (e.g., a bank, store, military base, computer system, automobile, home security system, or gate). *Id.* at 10:l, 24–28.

A registered person carries battery powered personal identification device (PID) 6 (e.g., similar in size to a hand-held pager), which includes biometric sensor 11. *Id.* at 10:28–11:5. Memory 20 stores an ID code that is set in PID 6 by the manufacturer. *Id.* at 11:11–13. The owner of PID 6

enrolls into the unit by scanning a finger using biometric sensor 11 to create an image that is stored as the fingerprint template in memory 20. *Id.* at 11:14–20, 15:30–16:6. PID 6 communicates wirelessly via transmission signal 41 with host facility 4. *Id.* at 12:14–16.

Host facility 4 is part of host system 30 (e.g., a bank ATM system or point of sale system), which also includes host processing unit 32. *Id.* at 11:31–12:2. "Host processing unit 32 may be located with host facility 4, or may be located at a remote location, where it may also serve other host facilities 4 in a distributed network 42." *Id.* at 12:3–5. "Memory 36 stores ID codes of enrolled individuals who have registered with host system 30." *Id.* at 12:6–7.

Figure 7 of Scott is reproduced below.

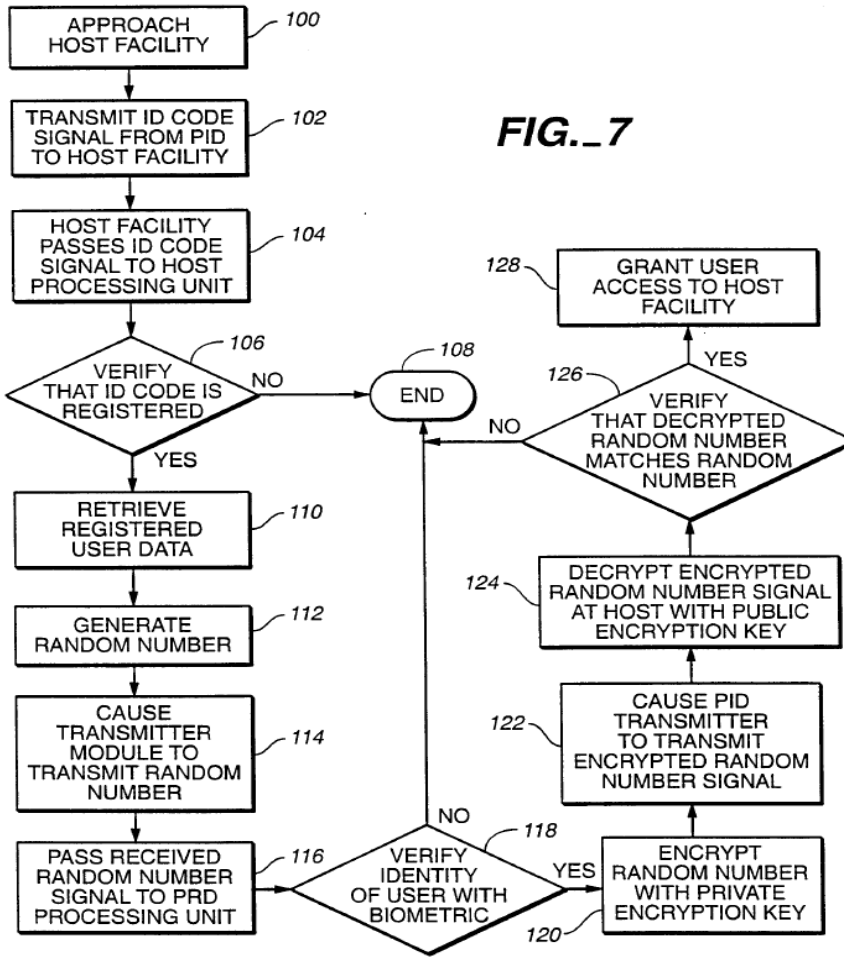


FIG._7

Figure 7 is a flow diagram of a method of accessing a host facility with a personal identification device. *Id.* at 10:13–14.

A user with PID 6 approaches host facility 4 (e.g., an ATM) and transmits the ID code to host receiver module 38, which passes it to host processing unit 32. *Id.* at 17:20–27 (steps 100–104). Host processing unit 32 verifies that the received ID code represents a registered ID code and, if so, the account or user information is located. *Id.* at 17:27–30 (steps 106, 110). Host processing unit 32, via transmitter module 40, sends a random number to PID 6, in response to which PID 6 performs a user verification. *Id.* at 18:1–4 (steps 112–118). PID 6 verifies the user's fingerprint when the user places their finger on platen 15 of biometric sensor 11 by comparing the

fingerprint signal to the stored fingerprint template. *Id.* at 16:19–29. If PID 6 successfully verifies the user's fingerprint, PID 6 encrypts the random number and sends it back to host processing unit 32, which decrypts the random number and verifies that it matches the random number it sent to PID 6. *Id.* at 18:5–14 (steps 120–126). If the random number is a match, host processing unit 32 grants the user access to host facility 4. *Id.* at 18:14–15 (step 128).

### 2. *Lapsley*

Lapsley describes "a system and method of using biometrics for processing electronic financial transactions such as on-line debit, off-line debit and credit transactions without requiring the user to directly use or possess any man-made tokens such as debit or credit cards or checks." Ex. 1007 ¶ 2.

Figure 2 of Lapsley, reproduced below, illustrates an example.

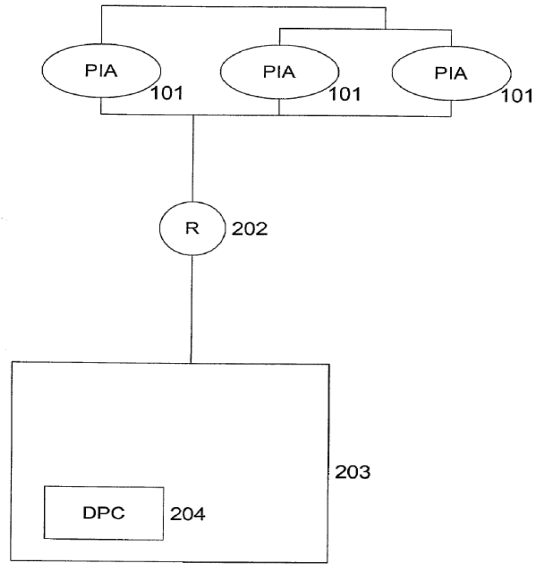


Figure 2 is a block diagram showing the connections among Party Identification Devices (PIAs) 101, router 202, and Network Operations Center (NOC) 203. *Id.* ¶ 47. Figure 2 is in the context of a supermarket

chain or other multi-lane retail chain with multiple PIAs 101 connected via an in-store local area network to local router 202, which is connected to NOC 203 via frame relay lines. *Id.* ¶ 98. NOC 203 includes Data Processing Center (DPC) 204. *Id.*

Each PIA 101 has a hardware identification code that is assigned to it and registered with DPC 204 at the time of manufacture, making the PIA uniquely identifiable to DPC 204 in transmissions from the PIA. *Id.* ¶¶ 85, 161. An entity uses the PIA hardware identification code to identify itself to the DPC. *Id.* ¶ 158.

Figure 7 of Lapsley is reproduced below.

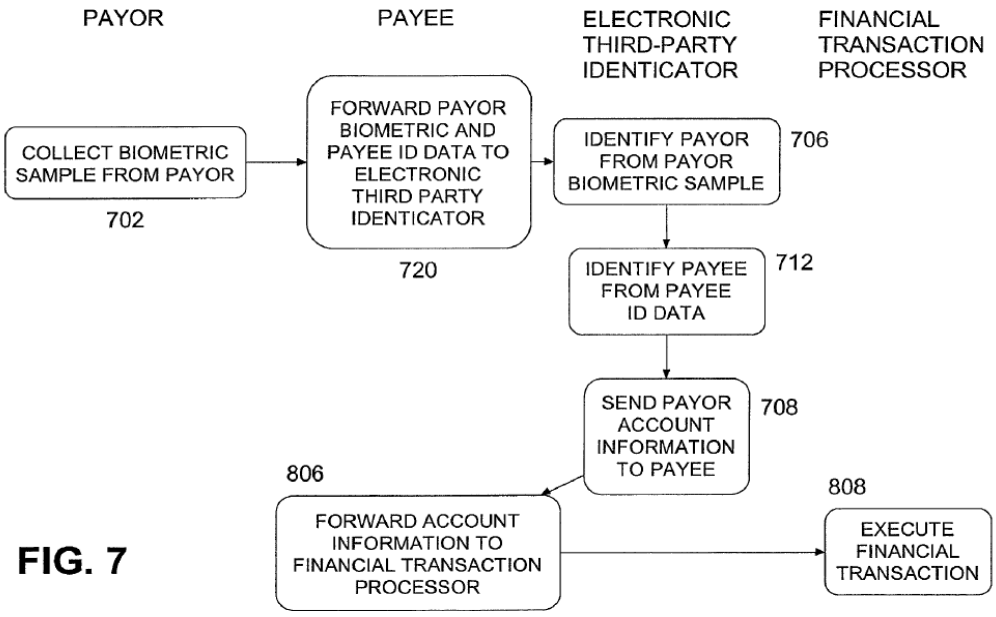


**FIG. 7**

Figure 7 is a flow diagram showing a transaction flow among the participants in a retail point-of-sale transaction. *Id.* ¶¶ 52, 166.

The customer/payor originates an electronic payment at a point-of-sale by submitting a bid biometric sample obtained by a biometric sensor of the PIA controlled by a payee/seller. *Id.* ¶¶ 166–167 (step 702). The PIA determines that the sample is not fraudulent and sends the sample to the DPC. *Id.* ¶ 167. The payor enters a PIN code into the PIA, and the

PIA transmits the biometric data, PIN, and hardware identification code of the PIA to the DPC. *Id.* ¶ 168 (step 720). The DPC identifies the payor using the biometric sample, retrieves a list of financial accounts that the payor has registered with the system, and transmits the list to the PIA. *Id.* (steps 706, 708). The DPC identifies the payee using the PIA hardware identification code. *Id.* ¶¶ 166, 168. The payor selects a financial account at the PIA, and the PIA transmits the financial information to the payee's in-store payment system (e.g., point-of-sale terminal or electronic cash register). *Id.* ¶¶ 169–170. The in-store payment system authorizes the transaction. *Id.* ¶ 170.

*3. Claim 1*

Petitioner argues that Scott and Lapsley collectively teach all of the limitations of claim 1. Pet. 19–26. With respect to the preamble of claim 1, Petitioner contends that Scott teaches a method of verifying a user during authentication of an integrated device (i.e., PID 6). *Id.* at 19.

With respect to limitation A, Petitioner argues that Scott teaches persistently storing "biometric data of a user" in memory 20 of PID 6 and persistently storing a plurality of codes and other data values including an ID code that uniquely identifies PID 6, where the ID code may be set by the device manufacturer and can be the device serial number. Pet. 20–21 (citing Ex. 1005 4:1–18, 6:28–7:23, 8:13–22, 11:11–20, 13:10–15, 15:30–16:6, 19:30–32).

With respect to limitation B, Petitioner argues that Scott discloses receiving a request for a biometric verification of the user by pressing a "verify" button on PID 6, and in response to this request, PID 6 can receive scan data from a biometric scan, such as a fingerprint scan from the user

placing a finger on platen 15, a voice biometric scan, "or any other type of biometric scan." Pet. 21–22 (citing Ex. 1005, 3:21–32, 16:19–29, Fig. 4A).

With respect to limitation C, Petitioner argues that Scott discloses that after receiving the biometric scan data, PID 6 compares the received biometric scan data (e.g., voice, iris, or fingerprint biometric) to a stored biometric template in order to verify the user's identity. Pet. 22 (citing Ex. 1005, 15:30–16:29).

With respect to the first portion of limitation D, Petitioner relies on the teachings of Scott. Pet. 22–23. As to the limitation of "responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code," Petitioner contends that, in response to the comparison discussed in connection with limitations B and C above, Scott's PID 6 wirelessly transmits to host facility 4 "an encrypted message with [the] ID code and other data such as a synchronization counter." *Id*. (citing Ex. 1005, 4:6–18, 5:22–6:24, 6:28–7:23).

With respect to the second portion of limitation D, namely "for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority," Petitioner contends that "Scott discloses that the third-party trusted authority host processing unit 32 stores a list that includes an ID code and a public key for each registered PID 6," and host processing unit 32 compares the device ID code received from PID 6 to this list to authenticate PID 6 as a legitimately registered device. *Id*. at 23–24 (citing 5:10–21, 6:11–21, 7:24–8:4, 8:18–22; 9:23–25, 11:12–13, 12:6–13, 13:10–15, 19:18–20, 30–32, Fig. 1). Although not cited in the Petition, Dr. Wolfe repeats these arguments in his testimony. *See* Ex. 1003 ¶ 45. Petitioner and Dr. Wolfe thus identify Scott's host processing unit 32 as corresponding to the claimed

"third-party trusted authority." Also, in its analysis of limitation E of claim 1, Petitioner makes clear that host facility 4 is the application (e.g., key card entry, ATM machine, garage door opener) that is accessed when the transaction is completed. Pet. 26 (citing Ex. 1005, 17:20–18:19, 5:10–21, 8:5–12).

Patent Owner argues that "host processing unit 32 is *part of* the system being accessed—it is not a third party." Prelim. Resp. 7 (citing Ex. 1005, 11:24–25, 11:30–12:1). As explained above, a "third-party trusted authority" is a trusted authority that is an entity separate from the parties to a transaction. *See supra* Section II.D. Scott describes both host processing unit 32 (the alleged "third-party trusted authority") and host facility 4 (the alleged application to be accessed by the user, "selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file") as part of a single entity, host system 30. Ex. 1005, 11:31–12:5 ("Host facility 4 is part of a host system 30. Host system 30 will typically be bank ATM systems, point of sale systems, and the like. Host system 30 also includes a host processing unit 32, which has a processor circuit 34 and memory 36 . . . . Host processing unit 32 may be located with host facility 4, or may be located at a remote location, where it may also serve other host facilities 4 in a distributed network 42."). As such, host processing unit 32, because it is not an entity separate from host facility 4, is not a third-party trusted authority.

Petitioner further argues that, "[t]o the extent [that Patent Owner] argues that Scott's host processing unit 32 is not a third-party trusted authority, Lapsley . . . provides additional disclosure rendering this feature of the limitation obvious to a [person of ordinary skill in the art]." Pet. 24.

Petitioner contends that Lapsley's DPC is a trusted third-party authority that receives biometric data and a hardware identification code from a PIA and uniquely identifies the PIA by finding the identification code on a list the DPC maintains. *Id.* at 24–25 (citing Ex. 1007 ¶¶ 54, 82, 85, 103, 104, 158, 161, 166–168).

Relying on Dr. Wolfe's testimony, Petitioner argues that a person of ordinary skill in the art

> would have been motivated to modify Scott's system such that authentication is performed by an external third-party trusted authority possessing a list of device ID codes that unique[ly] identify legitimate PIDs, as taught in Lapsley, to improve efficiency and flexibility of the system by consolidating ID codes to a central location at a secure third-party agent.

Pet. 25 (citing Ex. 1003 ¶ 47). Dr. Wolfe repeats this argument in his testimony, but does not state the basis for his opinion, rendering it of little value. *See* 37 C.F.R. § 42.65(a). Citing to Lapsley, Petitioner argues that an ordinarily skilled artisan "would have recognized the benefit in reducing the risk of fraud by improving security and authentication by using a trusted third-party agent to verify devices involved in a transaction." *Id.* (citing Ex. 1007 ¶¶ 8, 9, 27, 29). Petitioner argues that an ordinarily skilled artisan "would have further understood that it was common to have an ATM that is not owned by a bank use the bank as a third party for authorization and it was common for a store to use a bank or credit card exchange as a third party for authorization." *Id.* at 26. Petitioner does not cite any evidence for this argument.

Patent Owner responds that "Lapsley's DPC is part of the system providing access to a user's registered financial accounts, *i.e.*, a cloud based digital wallet—not a *third party* trusted authority." Prelim. Resp. 8 (citing

Ex. 1007 ¶¶ 102, 138, 139). Patent Owner contends that, "[i]n Lapsley, instead of using a personal fob or phone to access the DPC digital wallet, the user utilizes a Party Identification Apparatus located at a store." *Id.* at 8–9 (citing Ex. 1007 ¶¶ 167–169). According to Patent Owner, "[a]s the DPC is accessed with the PIA to retrieve a list of user financial accounts stored in the DPC, the DPC must be the system being accessed/authenticated. Consequently, Lapsley's DPC is not what the Petitioner and Patent Owner agree constitutes a 'third-party trusted authority.'" *Id.* at 9.

We agree with Patent Owner. Petitioner has not explained sufficiently why Lapsley's DPC is a third-party trusted authority, what entities the DPC is a third-party relative to, or what application the user is being permitted to access in the asserted combination. As Patent Owner points out, the DPC appears to be what is being accessed, as the payee and payor, with the PIA, access a list of financial accounts from the DPC. *See id.* at 8–9; Ex. 1007 ¶¶ 167–170. Here, the DPC is the resource to be accessed, but it is a party to the transaction, rather than a third party. This is similar to the situation Petitioner argues that the applicant distinguished during prosecution: "[d]uring prosecution, the applicant explained a 'user []prov[ing] to the same institution that authenticates the fingerprint information that the user is who he purports to be' does not satisfy the 'third party' limitation." *See* Ex. 2001, 7 (quoting remarks made by the applicant during prosecution of the related patent (alterations by Petitioner)).

Petitioner's reasons to combine also are conclusory and unsupported by persuasive evidence. In particular, Dr. Wolfe merely repeats Petitioner's arguments in his testimony, without further explaining them or identifying

the basis for his opinions.[10] *See* Ex. 1003 ¶ 48. We agree with Patent Owner that Petitioner has not shown that Lapsley teaches a "third-party trusted authority" or that a skilled artisan would have had reasons, with rational underpinning, to combine the teachings of Scott and Lapsley.

Because Petitioner does not show persuasively that either Scott or Lapsley teaches a "third-party trusted authority," as recited in claim 1, or that an ordinarily skilled artisan would have combined the teachings of those references, Petitioner has not shown sufficiently that Scott and Lapsley teach limitation D:

> responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority.

Petitioner's ground fails for an additional reason as well. The claim plainly requires that the access message be received "from the third-party trusted authority," per limitation E.

Petitioner argues that "in response to authentication of the received ID code by comparing it to a stored ID code, the receiver module 26 of PID 6 receives a random number signal from [host processing unit 32] that enables access to a secure resource." Pet. 26 (citing Ex. 1005, 5:10–21, 8:5–12, 17:20–18:19). Petitioner does not provide any further explanation as to why Scott's host processing unit 32 allegedly constitutes a "third-party trusted authority." *See id.* Nor does Petitioner mention Lapsley, or the combined teachings of Scott and Lapsley, in addressing limitation E of claim 1. *See id.* Because Petitioner has not shown sufficiently that host processing unit 32 is

[10] Moreover, as explained below, the entirety of Dr. Wolfe's testimony lacks credibility and is entitled to little or no weight. *See infra* Section II.G.

a "third-party trusted authority," Petitioner likewise has not established that Scott's random number signal is an "access message [sent] from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code," as recited in limitation E of claim 1. *See* Prelim. Resp. 9.

Therefore, Petitioner has not shown a reasonable likelihood of prevailing on its assertion that claim 1 is unpatentable over Scott and Lapsley.

*4. Claims 3–10 and 12*

Independent claim 9 recites the same elements of independent claim 1, discussed above, that we determine that Petitioner's Petition has not shown according to this ground of unpatentability. *See* Ex. 1001, 10:54–11:3. Claims 3–8 and 10–12 ultimately depend from claim 1. For the reasons explained above regarding claim 1, Petitioner has not shown a reasonable likelihood of prevailing on its assertion that claims 3–10 and 12 are unpatentable over Scott and Lapsley.

*F. Obviousness Ground Based on Scott, Lapsley, and Robinson*

Petitioner contends that claims 2 and 11 are unpatentable over Scott, Lapsley, and Robinson under 35 U.S.C. § 103(a). Pet. 34–36. Claims 2 and 11 ultimately depend from claim 1. Petitioner does not argue that the additional reference (Robinson) teaches the missing limitations of parent claim 1, as discussed above. *See id.* Accordingly, for the reasons explained above, Petitioner has not shown a reasonable likelihood of prevailing on its assertion that claims 2 and 11 are unpatentable.

*G. Obviousness Ground Based on Berardi, Shreve, and Kinoshita*

Petitioner contends that claims 1, 3–7, 9, 10, 12 are unpatentable over Berardi, Shreve, and Kinoshita under 35 U.S.C. § 103(a), citing the testimony of Dr. Wolfe as support. Pet. 36–46 (citing Ex. 1003).

Petitioner's allegations and citations to Berardi do not correspond to the disclosure of that reference. *See* Prelim. Resp. 10 ("With regard to Berardi, Petitioner references elements and paragraphs not contained within Berardi at all, *i.e.*, in error.").[11]

For example, in alleging that Berardi teaches "responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority," as recited in limitation D of claim 1, Petitioner argues that "issuer system 1010 [that] includes an issuer account server (IAS) 1014 that processes fob identifying information," of Berardi, corresponds to the claimed "third-party trusted authority." Pet. 38–39 (citing Ex. 1010, 10:56–11:12, 22:1–41, 28:50–67). Berardi does not describe an "issuer system 1010" or "issuer account server (IAS) 1014." The cited material in columns 10 and 11 is inapposite (and does not discuss issuer system 1010 or IAS 1014), Berardi ends its disclosure at line 30 (not line 41) of column 22, and column 28 does not exist in Berardi. Additionally, following the normal

[11] Patent Owner notes that Petitioner's errors "make[] it difficult to ascertain Petitioner's argument[s]," but argues that "a full reading of Berardi makes clear that it fails to disclose a 'third-party trusted authority.'" Prelim. Resp. 10. Patent Owner then presents substantive arguments as to Berardi, Shreve, and Kinoshita. *Id.* at 10–15. We deny the Petition as to this ground based on Petitioner's failure to present an understandable case as to Berardi and do not reach Patent Owner's additional arguments.

numbering of elements in patent drawings, the highest number referenced in Berardi is "906," short of the elements "1010" and "1014," discussed by Petitioner.

Also in its analysis of limitation E of claim 1, Petitioner states that Berardi discloses that "in response to authentication of the received identifying information of the fob 102, the POS device 110 may send 'an optical and/or audible transaction status message' to the RFID reader 104 for communication directly with the customer." Pet. 40–41 (citing Ex. 1010, 20:51-62, Fig. 8). Column 20, lines 51–62 of Berardi encompass a portion of claim 1 of Berardi, and the cited section does not discuss POS Device 110. Figure 8 of Berardi provides a flow diagram of an exemplary payment/transaction process, but does not detail sending an optical and/or audible message, as Petitioner alleges. We conclude that Petitioner did not simply misidentify or mislabel the components of Berardi it sought to reference.

There are numerous similar errors. For example, Petitioner relies on column 28, lines 50–67, which does not exist in Berardi, for limitations A, B and D of claim 1. *See* Pet. 37–39. Petitioner's citation to column 12, lines 36–41 in its analysis of limitation B of claim 1 does not correspond to biometric information, or anything else we can discern to be relevant to these limitations. *See id.* at 38. Instead, it discusses RFID reader 104 authenticating fob 102. Ex. 1010, 12:36–41. We do not intend to list all such errors here. We decline to speculate as to what Petitioner might have intended to cite. The result of the errors in the Petition is that we are unable to understand Petitioner's allegations and Patent Owner cannot fairly be said to be on notice of Petitioner's challenge based on Berardi.

Petitioner contends that (1) to the extent Berardi fails to teach limitation D of claim 1, Shreve provides additional disclosure; and (2) to the extent Berardi fails to teach limitation E of claim 1, Kinoshita provides additional disclosure. Pet. 39–41. However, because Petitioner has not sufficiently explained its allegations as to Berardi, it is impossible to understand Petitioner's proposed combination with Shreve and Kinoshita. Moreover, as explained above, Petitioner's arguments regarding limitations A, B, D, and E of claim 1 are based largely on material that does not exist in Berardi. Thus, even if we were able to discern Petitioner's arguments for limitations A, B, D, and E of claim 1, Petitioner's cited evidence does not support its allegations for other elements of claim 1.

Petitioner's allegations for independent claim 9 largely track or refer back to its analysis of claim 1 and, thus, suffer from the same defects. *See* Pet. 44–46. Petitioner's allegations for dependent claims 3–7, 10, and 12 do not shed any additional light on what Petitioner might have intended for claim 1, and instead largely cite irrelevant or non-existent material in Berardi. *Id.* at 42–44, 46.[12]

[12] We also express concern with Dr. Wolfe's testimony. Paragraphs 71–97 of his declaration (Exhibit 1003) appear to be a near carbon copy of pages 36–46 of the Petition, and include the Petition's citations to obviously incorrect or non-existent material in Berardi. These circumstances suggest a lack of attention, as even a cursory review would have shown that his testimony regarding Berardi includes numerous references to irrelevant or non-existent material, rendering that testimony not useful. This is not an instance of one or even a few inadvertent errors that might go missed upon a diligent review. The entirety of Dr. Wolfe's testimony regarding Berardi is defective on its face. For these reasons, the entirety of Dr. Wolfe's testimony lacks credibility and is entitled to little or no weight.

In sum, we cannot discern Petitioner's allegations of obviousness based on Berardi, Shreve, and Kinoshita, nor can we say Patent Owner is on notice of those allegations. Accordingly, Petitioner has not shown a reasonable likelihood of prevailing on its assertion that claims 1, 3–7, 9, 10, 12 are unpatentable over Berardi, Shreve, and Kinoshita.

## III. CONCLUSION

Based on the arguments presented in the Petition, we conclude that Petitioner has not demonstrated a reasonable likelihood of prevailing with respect to at least one claim of the '905 Patent challenged in the Petition. Therefore, we do not institute an *inter partes* review.

## IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that the Petition is denied and no *inter partes* review is instituted.

FOR PETITIONER:

James M. Glass
Marissa Ducca
Richard Lowry
Sean Gloth
QUINN EMANUEL URQUHART & SULLIVAN, LLP
jimglass@quinnemanuel.com
marissaducca@quinnemanuel.com
richardlowry@quinnemanuel.com
seangloth@quinnemanuel.com

FOR PATENT OWNER:

David L. Hecht
James Zak
HECHT PARTNERS LLP
dhecht@hechtpartners.com
jzak@hechtpartners.com